A little tour in the little world of passwords stealers

Paul Jung
CERT - XLM

EXCELLIUM

Your first call when it comes to IT and security

TLP:White
What is a PWS

Av’s industry says…

• Password Stealer
• PaSSWord
• Information Stealer
What can it steal?

- Credentials in browser
- Credentials in configuration files/registry
- Coin Wallets
- Serial numbers

Everything mainly in user land without auth.
What can it steal?
PWS Objectives

Optionally…

• Grab screenshots

• Key logging
How it works (usually)

- Buy the tool, or find an open / cracked one
How it works (usually)

• Forums or Yt are full of nice ads…
AutoLOG kills a total of 182 AntiVirus and Anti-Malware processes, of which some notable ones are:

- AVG AntiVirus
- Ad-Aware
- ArcaVir Internet Security
- Avast AntiVirus
- Avira AntiVir
- BitDefender
- BullGuard
- Clam AntiVirus
- Comodo AntiVirus
- Dr. Web
- ESET NOD32
- Emisoft: Anti Malware
- F-Prot AntiVirus
- F-Secure AntiVirus
- FSB AntiVirus
- FortiClient
- ICBit Malware Fighter
- Ikarus Security
- Immunet Plus
- K7 Ultimate
- Kaspersky Internet Security
- KeyScrambler
- KingSoft AntiVirus
- MalwareBytes Anti Malware
- McAfee Security Suite
- NANO AntiVirus
- NetGate
- Norman AntiVirus
- Norton 360
- Norton Internet Security
- Outpost Security
- Ozone AV
- Panda AntiVirus
- QuickHeal
- Solo AntiVirus
- Sophos AntiVirus
- Super AntiSpyware
- Total Defense AntiVirus
- Trend Micro Titanium AV
- TrustPort AntiVirus
- Twister AntiVirus
- VBA32 AntiVirus
- Vipre AntiVirus
- Zoner AntiVirus
- eScan AntiVirus
- eTrust AntiVirus
- nProtect
- G Data
How it works

Forums are full of nice ads…
Since the primary password recovery tool may be a bit heavy including all those passwords recovered, we have provided an alternative compact password recovery tool so that you can use it for your convenience, as well as for lowering the stress on the system. No other keylogger offers such a feature

- Google Chrome (All Versions)
- Microsoft Outlook (All Versions)
- Mozilla Firefox (All Versions)
- Mozilla Thunderbird (All Versions)
- FileZilla (All Versions)
- No-IP (All Versions)

**PRODUCT KEY**

AutoLOG also has an option of recovering product keys from popular entertainment media and games such as:

- AutoCAD
- Adobe Acrobat
- Adobe Photoshop
- Nero
- Visual Studio
- CorelDraw
- Call of Duty
- Battlefield
- Splinter Cell
- Command & Conquer
- Crysis
- Counter Strike
- FIFA
- IGI 2
- Medal of Honor
- Need for Speed
- SimCity
- The Sims

Further features include a cookie stealer which can be used to hijack active sessions and a Skype chat history stealer with full logs of each conversation with each contact.
How it works (usually)

**Strong Keylogger:**
AutoLOG has multiple keylogging methods and features a strong & persistent keyboard hook which will record ever keystroke typed.

**Cookie Stealer:**
AutoLOG is one of the very few keyloggers which present a function to steal user cookies which can be used for effective session hijacking.

**Skype Chat History Stealer:**
For the first time in history, we present a keylogger that has such a function. This skype chat history stepper will grab the chat db in a readable format with all relevant info included.

**Screenshot Trigger:**
This unique feature, exclusive to AutoLOG gives you a mechanism where the screenshot logger will rapidly take screenshots when a certain window is opened.
How it works (usually)

• And they’re plenty of those.
Plenty of those...
Plenty of those...
How it works (usually)

• Composants

• Builder
How it works (usually)

• Composants
• Builder
How it works (usually)
How does it come (usually)
Panel

- A couple of them need a php panel
Quality is not constant

- JPro Crack Stealer
- Predator Pain
- Pony
- AutoLog
- Agent Tesla
JPro Crack

The “opportunistic” one
JPro Crack

- Diagnostic wallet for truck engine
- From Noregon
- Cracks are available on forums
- Not all cracks are working well
JPro Crack

- Steal creds
- Firefox
- Google Chrome
- Opera Browser
- Pidgin
- Thunderbird
- FileZilla
- Proxifier
JPro Crack

- Detect av’s and firewall through WMI
- root\SecurityCenter
- SELECT * FROM FirewallProduct
- SELECT * FROM AntiVirusProduct
JPro Crack

- Report in clear txt
- in an ugly way
JPro Crack
JPro Crack

06-07-2017, 09:24 PM

DetroitTech1980
Location Offline
Senior Member

Post: #7

RE: Noregon JPRO Commercial Fleet Diagnostics 2016 v2.3 + Crack

Has anybody checked this and confirmed it work with ZERO virus?
Pony

The most “Famous”
Pony

- Named by Kaspersky and Microsoft as FareIT
- In the field since 2011, multiple versions
- Code is “open” now
- Builder in Delphi
- Stealer in Assembler (MASM)
Pony

- Used often as dropper
- Try credentials to brute force local accounts
Pony

131
Pony

- Reports to “gate.php” using POST

- Ua by default
  
  “Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)”

- Basic security to avoid detection

... 

if (strlen($received_report_data) == 0) {
    // received empty report
    // return 404
    $pony_db->add_log_line('NOTIFY_GATE RECEIVED NULL REPORT',
        CLOG_SOURCE_GATE, null, $ip);
    header('HTTP/1.0 404 Not Found');
    header('Status: 404 Not Found');
    $_SERVER['REDIRECT_STATUS'] = 404;
    if (file_exists('404.html'))
        echo file_get_contents('404.html');
    die();
}
Predator Pain

The “Laziest”
Predator Pain

• In the field since 2008, multiple versions
• Written in .net
• Could report in http, smtp and ftp
Predator Pain

- Does not retrieve anything by itself!

[17:59]:[/~predator_pain/pp]/::
$decrrottePE.py sample.exe
[i] Scanning sample.exe
  >Seeking / Searching for PE
[*] Found PE_0.exe 517632 bytes saved
  >Seeking - Searching for PE
[*] Found PE_20804.exe 6656 bytes saved
  >Seeking / Searching for PE
[*] Found PE_27465.exe 345600 bytes saved
  >Seeking | Searching for PE
[*] Found PE_379310.exe 98816 bytes saved
  >Seeking / Searching for PE
Predator Pain

```csharp
40    return false;
41
42    if (lstring.IsNullOrEmpty(optionalArguments))
43    {
44        hostProcess = hostProcess + "" + optionalArguments;
45    }
46
48    {
49        return false;
50    }

51    IntPtr intptr = new IntPtr((int)(ptr4 + 52));
52    MemoryExecute.NtUnmapViewOfFileSection((IntPtr)array4[0], intptr);
53
54    if (MemoryExecute.VirtualAllocEx((IntPtr)array4[0], intptr, *(uint*)(ptr4 + 88), 12288u, 64u) == IntPtr.Zero)
55    {
56        this.Run(exeBuffer, hostProcess, optionalArguments);
57    }
58
59    fixed (byte* ptr9 = &exeBuffer[0])
60    {
61        MemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], intptr, *(IntPtr*)((void*)ptr9), *(uint*)(ptr4 + 84), IntPtr.Zero);
62        for (ushort num2 = 0; num2 < *(ushort*)(ptr4 + 6); num2 += 1)
63        {
64            Buffer.BlockCopy(exeBuffer, num + array2.Length + array.Length * (int)num2, array, 0, array.Length);
65            fixed (byte* ptr10 = &exeBuffer[(int)((UIntPtr*)((uint*)(ptr2 + 20)))]
66            {
67                MemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], (IntPtr)((long)((int)intptr) + (long)(*(ulong*)(uint*)(ptr2 + 12)))), *(IntPtr*)((void*)ptr10), *(uint*)(ptr2 + 16), IntPtr.Zero);
68            }
69        }
70
71    }
72
73    MemoryExecute.NtGetContextThread((IntPtr)array4[1], (IntPtr)((void*)ptr8));
74    MemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], (IntPtr)((long)((long*)((uint*)(ptr8 + 172)))), intptr, 4u, IntPtr.Zero);
75
76    *(int*)(ptr8 + 176) = *(intptr + (int*)((uint*)(ptr4 + 40)));
77    MemoryExecute.NtSetContextThread((IntPtr)array4[1], (IntPtr)((void*)ptr8));
78    MemoryExecute.NtResumeThread((IntPtr)array4[1], IntPtr.Zero);
79
80    return true;
```
Predator Pain

- It loads and executes recovery tools from memory
Predator Pain

• Configuration is ciphered with DES/AES

• It reports with “GET”

[URI]?fname=[FILENAME]&data=[DATA]
AutoLog

Another “less Lazy”
AutoLog

- In the field since 2016
- Autolog is written in AutoIT
- Seen packed in .NET
- Painfull as a Javascript :)
AutoLog

Obfuscated AutoIT code

Data file

FIRST’2018
Global $a536080041c = a4600006061($cw[1]), $a1a60a05f4c = a4600006061($cw[2]), $a0660b02754 = a4600006061($cw[3]), $a5e60c01e15 = a4600006061($cw[4]), $a2460d0140a = a4600006061($cw[5]), $a1660e03a06 = a4600006061($cw[6]), $a1560f02d5e = a4600006061($cw[7]), $a2e70000721 = a4600006061($cw[8]), $a3270202010 = a4600006061($cw[9]), $a397040024d = a4600006061($cw[10]), $a507060060e = a4600006061($cw[11]), $a0870800826 = a4600006061($cw[12]), $a1970a04f0b = a4600006061($cw[13]), $a4270c06247 = a4600006061($cw[14]), $a5470e03d0a = a4600006061($cw[15]), $a2b80001d00 = a4600006061($cw[16]), $a108020631a = a4600006061($cw[17]), $......
Func a4600006061($a4600006061)
  Local $a4600006061_
  For $x = 1 To StringLen($a4600006061) Step 2
    $a4600006061_ &= Chr(Dec(StringMid($a4600006061, $x, 2)))
  Next
  Return $a4600006061_
EndFunc
AutoLog

- Autoit has an **eval()** function

```
$a5ef8203511 = Execute($a59f8303224) & $a15f8403357 & Execute($a1bf8506331) & $a51f860605b & Execute($a3af8701028) & $a63f8805a42 & Execute($a57f890304f) & $a15f8a01c39 & Execute($a38f8b00c32) & $a1ff8c01c1b & Execute($a10f8d04920)
```
AutoLog

- Autolog takes regular screenshots
- Nice colourful key logger logs
- Communicates via SMTP
- AutoIT allows direct API call
  - It logs keys by using Dllcallback bind on keypress
AutoLog

Also Check for virtualisation by looking processes:

```cpp
if ProcessExists(a3a6050431b(a5a60605046($a0d1c701d59))) Then Exit ;

• VboxService.exe
• VMwaretray.exe
• vpc.exe
• VBoxTray.exe
• VmWareTools.exe
• VmwareService.exe
• VBoxexe
```
AutoLog

• Autolog does not retrieve passwords by itself
• Autolog downloads and uses “lazagne”

https://github.com/AlessandroZ/LaZagne
Agent Tesla

The “professional”
Agent Tesla

- AgentTesla is simply sold online
Agent Tesla

• But agent tesla is not a malware !!

**WHAT IS NOT.**

Agent Tesla is a software for monitoring your personal computer. It is not a malware. Please, don’t use for computers which is not access permission. Any use of the words "Slave", "Infect", "Bot", "Spread" or "Hack" will instantly cancel all your support, and if we have your username you will be banned.

**WHAT IS AGENT TESLA.**

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personal computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in log. You can receive your logs via e-mail, ftp or php(web panel).
Agent Tesla

• But agent tesla is not a malware !!
Agent Tesla

- Buy online in Bitcoin/Perfect money $12/m, $69/y
- .Net code
- Reports in smtp, ftp and http
- Builder is auto updating
- Crypter is part of the package (another painful .net)
- Macro based dropper is also part of the package
Agent Tesla

- POST to “api.php”
- Steals 33 applications
- Grab screens
- Decoy Messages
Agent Tesla

- Every string is ciphered using Industry standard.
  - PBKDF1 SHA1 Password derivation
    - using API .getbytes to upgrade key from 20 to 32 bytes.
  - AES 256 CBC
Agent Tesla

• It’s quite hard to audit the panel

• protected by Ioncube
Agent Tesla

• Luckily, security on panels is often weak…

/Screens
Agent Tesla

Last version:
https://www.agenttesla.com/version.html 3.2.52
Detection
## Classification

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Classification</th>
<th>Company</th>
<th>Confidence</th>
</tr>
</thead>
</table>
| Ad-Aware | Trojan Agent CNQR | Aeghi.ah | \\
| AhnLab-V3 | Trojan/Win32.InjectR21C7+6 | AL'ac | \\
| Antly-AVL | Trojan/Win32.5SGeneric | Arcabit | \\
| Avast | Win32:Malware-gen | AVG | \\
| Avira | TR/Downloader.covmws | AVware | \\
| BitDefender | Trojan.Agent.CQORB | CAT Quick Heal | \\
| Comodo | Unclassified Malware | CrowdStrike Falcon | \\
| Cybersecurity | malicious.1b9f7 | Qlance | \\
| Cyren | W32/Fareit.WJ/vA.2'23 | DrWeb | \\
| Emsisoft | Trojan.Injector:A | Endgame | \\
| eScan | Trojan.Agent.CQORB | ESET-NOE32 | \\
| F-Prot | W32/Fareit.CFI | F-Secure | \\
| Fortinet | Malicious_Behavior:SB | GData | \\
| Ikarus | Trojan.Cryot | Hangmin | \\
| K7 AntiVirus | Trojan (05S19aad1) | K7GW | Trojan (05S19aad1) |
| Kaspersky | Trojan-FSWWin32.Fareit.ini | Malwarebytes | Spyware.Leki80: |
| MAX | malware (all score = 100) | McAfee | Trojan-FNVNJ1C1.1583252528 |
| McAfee-CW-Edition | Trojan-FNWV:3Cl5:55235225 | Microsoft | Trojan.W32/Tigervh3ri |
| MADO AntiVirus | Trojan.Win32.Down.Ctucki | mProtect | Trojan/W32.Agent.657920.CP |
| Palo Alto Networks | generic:nd | Panda | \\
| Ohoo-360 | HEJR/CVM05.19334.Malware.Gen | Rising | Trojan Kryptik!AE18 (CLASSIC) |
| SentinelOne | static engine:malicious | Sophos AV | Trojan/Fareit-JTZ |

**FIRST'2018**
Classification

• A lot of yara rules already exist
  
  • https://github.com/Yara-Rules/rules

  • https://github.com/Th4nat0s/Yaramoi

• Need to be unpacked first!
Classification

- Auto unpack
- 32 bits
- RUNPE

https://github.com/Th4nat0s/Chall_Tools/blob/master/malwares/unpack_runpe.py
Classification

I hate .NET packers !!!

• Start > No Break > Debug > Modules
Classification

- RunPE! nice
Classification

- RunPE! nice... UPX... nice

`$file out.exe`
`out.exe: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed`
Classification

- Arghhh
Post Detection

- Some panels are easy to spot in your logs
  - **KEYBASE**
    - GET POST.PHP?TYPE=…&MACHINENAME=…
  - **LOKIBOT**
    - POST FRE[D]?[.]PHP
    - UA : (Charon; Inferno)
Post Detection

• DIAMOND FOX, PONY, HANCITOR or… ?

• GATE.PHP
Post Detection

- Most of them share the admin and reports

- Pony, Lockybot, Tesla etc… do that
Post Detection

• Most of them share the admin and reports
  
• Pony, Lockybot, Tesla etc... do that

$./c2id.py seek -u http://www.ctrhelpdesk.com/admin/Panel/five
2018-06-20 22:57:34,437 :: INFO :: No Root page found, brute forcing
2018-06-20 22:58:03,158 :: INFO :: Found Locky Bot at 100%

https://github.com/Th4nat0s/c2id
Post Detection

- Most of them share the admin and reports

- Pony, Lockybot, Tesla etc… do that

```yaml
$name: pony 2.2
root: admin.php, gate.php
rule:
  - page: config.php
code: 200
  - page: gate.php
code: 404
  - page: admin.php
code: 200
  - page: 'includes/templates/header.tpl'
code: 200
contains: '<div class="pony_hdr_text">Pony 2.2'
  - page: 'includes/design/images/favicon.ico'
code: 200
hash: b2e87bb6f28663fe5d28dec0d980d4cb
```
Thank’s

Thanks to all guys who track panels and have fun with it!

If you need/have info on stealer ping us

cert@excellium-services.com

www.excellium-services.com